

UNCLASSIFIED

AD NUMBER	
AD513154	
CLASSIFICATION CHANGES	
TO:	unclassified
FROM:	confidential
LIMITATION CHANGES	
TO:	Approved for public release, distribution unlimited
FROM:	Distribution authorized to U.S. Gov't. agencies only; Administrative/Operational Use; Oct 1970]. Other requests shall be referred to Director, Naval Research Laboratory, Washington, DC. 20390.
AUTHORITY	
NRL ltr, 7 Oct 2003; NRL ltr, 7 Oct 2003	

THIS PAGE IS UNCLASSIFIED

UNCLASSIFIED

AD NUMBER
AD513154
CLASSIFICATION CHANGES
TO
confidential
FROM
secret
AUTHORITY
31 Oct 1982, Group-3, per document marking

THIS PAGE IS UNCLASSIFIED

SECRET

NRL Memorandum Report 2186

Copy No.  of 100 Copies

AD513154

OSIS Security Implications

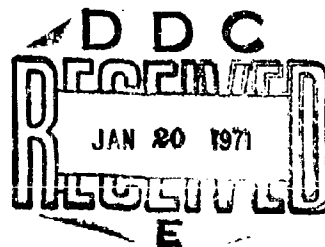
[Unclassified Title]

PAUL H. ASHLEY

Information Systems Group

Office of the Associate Director of Research for General Sciences

October 1970



NAVAL RESEARCH LABORATORY
Washington, D.C.

DDC CONTROL
NO10191

SECRET

Downgraded at 12 year intervals;
Not automatically declassified.

In addition to security requirements which apply to this document and must be met, each transmittal outside the agencies of the U.S. Government; must have prior approval of the Director, Naval Research Laboratory, Washington, D.C. 20390.

SECRET

SECURITY

This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, Title 18, U.S.C., Sections 793 and 794. The transmission or revelation of its contents in any manner to an unauthorized person is prohibited by law.

SECRET

SECRET

UNCLASSIFIED

CONTENTS

Abstract	ii
Problem Status	ii
Authorization	iii
Acknowledgment	
INTRODUCTION	1
SYSTEM GOALS AND FUNCTIONS	3
MAJOR COMPONENTS AND ORGANIZATIONAL CONCEPT	7
FUNCTIONAL INFORMATION FLOWS	12
SECURITY AND DATA CONTROL PROBLEMS	15
FUNCTIONAL PROCEDURES FOR EFFECTING SECURITY	20
REFERENCES	44
APPENDIX A - Security Doctrine	45
APPENDIX B - Security Considerations in OSIS Technical Development	64

This material contains information affecting
the national defense of the United States
within the meaning of the Espionage Laws
(Title 18, U.S.C. Sec. 793 and 794),
of which in whole or in part this person is

DOWNGRADED AT 10 YEAR
INTERVALS; NOT AUTOMATICALLY
DECLASSIFIED

002 CONTROL
10191

UNCLASSIFIED

UNCLASSIFIED

ABSTRACT

This report reviews the Ocean Surveillance Information System (OSIS) envisioned in draft SOR 35-15 and PTA 35-15T with particular attention to the security and data control problems. Alternative means of achieving multilevel security are discussed, and a software oriented task is proposed for the development of program modules in satisfaction of presently envisioned data security requirements. Current security doctrine is reviewed in Appendix A. A working paper on Security Considerations in OSIS Technical Development, which supports security aspects in the preparation of an OSIS Technical Development Plan, is provided in Appendix B.

PROBLEM STATUS

This study was conducted under NAVELEX OSIS tasking and this report constitutes the final report on the security phases of that task. The preparation of this report was partially supported by the NELC task and this report also constitutes the final report on that task. It is expected that additional work will be prosecuted on this problem under other NELC-assigned OSIS tasks.

AUTHORIZATION

NRL Problems B01-06 and B02-08
NAVELEX Subproject X3515
NELC Task N427-17

UNCLASSIFIED

SECRET

ACKNOWLEDGMENT

The author wishes to acknowledge the significant contribution of Dr. Bruce Wald for his perception and insight on the many security problems of an ocean surveillance information system; as well as his work in the development of the machine independent software module approach for meeting the system security requirements.

The paper on Security Considerations in OSIS Technical Development (Appendix B) includes Mr. Stanley H. Wilson's consideration of hardware/software problems related to OSIS security requirements, and contains material separately submitted which supported the preparation of the OSIS Technical Development Plan.

SECRET

UNCLASSIFIED

OSIS SECURITY IMPLICATIONS

I. INTRODUCTION (Unclassified)

Naval commands at various levels require information about activities on, above, and below the oceans in the conduct of their operations. A basic objective of the Ocean Surveillance Information System (OSIS) is to provide a complete, accurate, current picture of ocean oriented activities required for decision making in Naval operations. A portion of this up-to-date picture is based on classified ocean surveillance information received from sensors and other sources, which must be given a degree of security protection commensurate with its sensitivity. Users of this ocean surveillance information may include not only operational commands, but high level planners and other governmental agencies. Some of these users may require only current unclassified information that is generally available, while others require all the information held by the system, commensurate with their degree of security access. The system must respond to each query with complete information, limited only by the user's security clearance, access level, or other user imposed constraints.

To consider adequately the entire amount of sensor information and reports on ocean traffic that is available, and to provide timely information for operational decision makers, requires the total integration of the human with the machine which assists through the automation of many heretofore manual operations. Man can now concentrate his efforts in matters where his involvement is necessary, while the machine will perform many diverse tasks in the collecting, routing, correlating, and classifying of information. This automated

UNCLASSIFIED

conversion of diverse source data into command support information should allow the human to give maximum attention to the analytic function, where his judgment, reasoning, and experience, will contribute to a more effective evaluation of the information.

The OSIS system will provide timely information to tactical Naval commanders in all geographical areas while also being responsive to top level management where national policy and strategic planning considerations are most significant. Special consideration will be given to initial classification and correlation requirements at the operational user level, while continuing to provide a viable system responsive to the demand of top level decision makers.

SECRET

II. SYSTEM GOALS AND FUNCTIONS (Secret)

The system is predicated on a capability to provide all levels of command with surveillance information on surface, sub-surface, and airborne vehicles which are detected in the ocean areas throughout the world. Major goals of the OSIS development are:

1. To disseminate operational intelligence information through the Fleet Ocean Surveillance Information Centers (FOSICs) to fleet users at all command echelons in a timely manner in order to permit command decisions to be made in tactical situations.
2. To provide information through the National Ocean Surveillance Information Center (NOSIC) in an expeditious manner, for use in strategic planning at national command levels.

Many of the OSIS functions will support both system goals; however, the time constraints on the system for tactical demands may vary widely from the strategic requirements. The tactical user requires information with a fast response time for making immediate decisions affecting ongoing operations. Any essential information should be available to the operational user from a FOSIC as required by the immediate needs of an ongoing tactical operation.

The NOSIC requires timely complete information for strategic planning at the highest levels. All the FOSIC's data are processed with other special information available to the NOSIC for this purpose.

SECRET

Some of the functional requirements of OSIS, as specified in SOR 35-15* include:

1. The acquisition, correlation, processing and evaluation of ocean surveillance information from all sources.
2. Incorporation of Special Intelligence data as required to complete the information needs of the system's users.
3. A capability to display all targets within a specified radius of a given point, on demand.
4. Maintenance of current data bases at all Centers. Provision of urgent information at precedence required for tactical users.
5. Maintenance of diverse files such as ships characteristics, historical matters, environmental matters, optimum route generation for shipping, etc.
6. Provision of timely reports on intelligence indications and evaluations, maritime activities, trends and other significant activities of the ocean areas.

There is a close mutually supporting functional relationship between FOSIC's and the NOSIC which must be considered when examining system security needs. The FOSIC's are a principal data support source for the National Center which maintains a total data base either within the Center or by an update and query capability to the Fleet Centers. These functional relationships are described in

*SOR 35-15 (Draft), as revised 27 July 1970.

SECRET

PTA 35-15T and are outlined in Fig. 1 as background on subsequent discussion of security and data control problems.

The designations NOSIC and FOSIC are used with reference to the development of an ocean surveillance system for the intelligence community; while SOR 35-15 uses the terms World-Wide Center and Regional Centers in a similar context. Although the terms are synonymous at this stage of development, one should be aware that the intelligence oriented development could result in a restricted access system or subsystem; as contrasted to a more accessible OSIS, which could provide unclassified information to some users, as well as classified information to other users meeting the access requirements for particular material.

SECRET

FOSIC

1. Acquires, collates, correlates ocean surveillance information from all regional sources.
2. Updates regional data base.
3. Provides update to NOSIC data base.
4. Provides subscribers with tactical intelligence having immediate or short term bearing on operations.
5. Provides urgent information to tactical commanders in real time.
6. Display and provide NOSIC with all unidentified contacts.
7. Display position, course, speed, and tracks of contacts in area. Provide to NOSIC on demand.
8. Maintain file of ships characteristics, sailing plans and other relevant shipping information.

NOSIC

1. Accepts regional information from all regions which is correlated and processed with other source information available to the Center.
2. Updates NOSIC all source data base.
3. Provides users with strategic and tactical intelligence.
4. Provides urgent information to users/subscribers in real time.
5. Provides users/subscribers with maritime activity reports, trends, activity patterns, etc.
6. Display and provide Regional Centers with special information on activity in area-not detected by region.
7. Maintain file of ships characteristics, sailing plans and other relevant information.

Figure 1.- Mutually Supporting Responsibilities

SECRET

III. MAJOR COMPONENTS AND ORGANIZATIONAL ENVIRONMENT (Secret)

The OSIS system consists of a world-wide network of Ocean Surveillance Centers, which provide information to users within regional areas for current operations, and to a National Center in the Washington area where all ocean surveillance information is received as required in the Nation's defense. Regional centers will be located adjacent to Naval commands in the Hawaii, San Francisco, Norfolk, and London areas. Each Center is expected to have its own data processing and display capability, together with requisite communications capabilities to link up with adjacent Centers as well as the National Center in Washington.

SYSTEM COMPONENTS (Secret)

National Center

The National Center will maintain analytical coverage of ocean surveillance activities on a world-wide basis, while FOSIC's will generally confine the scope of their analysis to the geographic areas for which they are responsible. It is anticipated that Fleet Centers will maintain a data base which includes their own and an adjacent region.

The National Center will not only receive inputs of correlated information from the various FOSIC's, but will also be the primary recipient of information from other Washington area governmental agencies. Some of these inputs will be special category or sensitive information. Expeditious decisions are required when processing National Center items affecting current operations in order to provide regions and on-scene commanders with the information needed to influence the outcome of tactical operations. Primary control of sensitive

SECRET

information may be vested in the NOSIC, however Fleet Centers would have access to all categories of information including sensitive intelligence affecting their region. The decision to provide sensitive information to subscribers, e.g., tactical commander, type commanders, etc., must be made by either a FOSIC or the NOSIC as circumstances dictate. The NOSIC would have access to regional data bases, and the Fleet Centers would have access to their regional information held by the National Center at all times.

Regional/Fleet Centers

FOSIC's will be responsible for initial receipt and processing of information received from Type Commanders and sensor systems closest to them. As this information is processed, it will be available to the NOSIC and to Regional subscribers, either when queried on-line or at intervals as required by standard operating procedures. Regional sensor systems would have a capability for the input of sensitive data (SI) to the FOSIC; however, access is not necessarily provided to this information from the subscriber level. When required for ongoing operations, sensitive information will be provided subscribers upon decision of either the NOSIC or the FOSIC concerned. Sensitive information held by a FOSIC will generally be limited to that Center's area of responsibility except when a Fleet Center assumes alternate Center responsibilities for the National Center.

User (Remote) Terminals

Remote terminals are expected to be available not only in the vicinity of the Centers, but also to operational commands, including Navy Type Commanders and individual ships in special cases. The physical security requirements for remote terminals, which have access to classified matter, are generally determined by the highest

SECRET

classification of information which may be accessed by users of the terminal. The Command responsible for a remote terminal must insure that the remote terminal area is secure from all personnel who do not have proper level of classification access and need to know.

The probable geographical separation of users and subscribers contributes to problems of identification of personnel, and in some cases to the identification of the remote terminal where dedicated communications links are not used. Authenticators or passwords provide a means of identification to the system which may be augmented by additional "keys" to determine access level of classification authorized as well as access to specific files at that level. Such authentication devices could be controlled by the NOSIC, where lists would be compiled at irregular intervals, and forwarded by separate secure communications systems to the command elements having users and subscribers to the system. Software which generates random authenticator lists is feasible; however, these lists could provide a penetration route to the entire system should they be compromised.

The operator's identity and qualifications for access or update of specific files may also be established through the use of keys or other access procedures. There is a possibility that material contained in files having a higher classification than the user's clearance may be relevant to a remote user's query. Rather than automatic exclusion of this special category data, a "flag" or signal to the security monitor indicating that a user is receiving only partial information to his query (because of classification limits) should be incorporated in the system. This partial information "flag" could serve to alert the human decision maker who would determine if additional information should be provided the user. An alternative means of providing essential special category information to the user would use sanitization techniques such as elimination of source, removal of credibility data, and other means to allow dissemination at a reduced classification level.

SECRET

(THIS PAGE UNCLASSIFIED)

NAVY ORGANIZATIONAL ENVIRONMENT (Unclassified)

The operational components of the Navy which need ocean surveillance information in the performance of their missions will have a marked influence on what capabilities must be provided by the Fleet Centers, and a lesser influence on the National Center requirements. An indication of functional information flows between the NOSIC, FOSIC's, and tactical subscribers is fundamental to the development of security measures for use in OSIS. This information flow implies a common conceptual base and performance standard for the system. Hardware must be compatible, and as practicable software for the system should be centrally designed and prepared.

A generalized system configuration which could be readily adapted to current organizational structure is depicted in Figure 2. Regional Centers would be responsible for collating, correlating and initial processing of the information provided by subordinate commanders, e.g., Type Commanders, ASW Forces, Submarine forces, as well as that received from separate regional sensor systems. A Regional Center would periodically and when queried, make its updated information available to the National Center, as well as tactical users within the region. Type Commands and other users with proper access would have a capability for on line query of the regional data base at any time. The National Center would normally receive special category or sensitive information, correlate it with other information at that level, and would have the responsibility for providing it to Regional Centers or to the "on scene" tactical user when necessary. Routinely, there would be no requirement for tactical users to access the World Wide Center data base, since they would have direct access to the regional data base, and alternate access through an adjacent type command in event of loss of their own data base. A designated Type Commander in the region would be expected to assume duties as alternate Regional Center, in event of casualty, and in this role would be the only regional TYCOM with access to the World Wide Center.

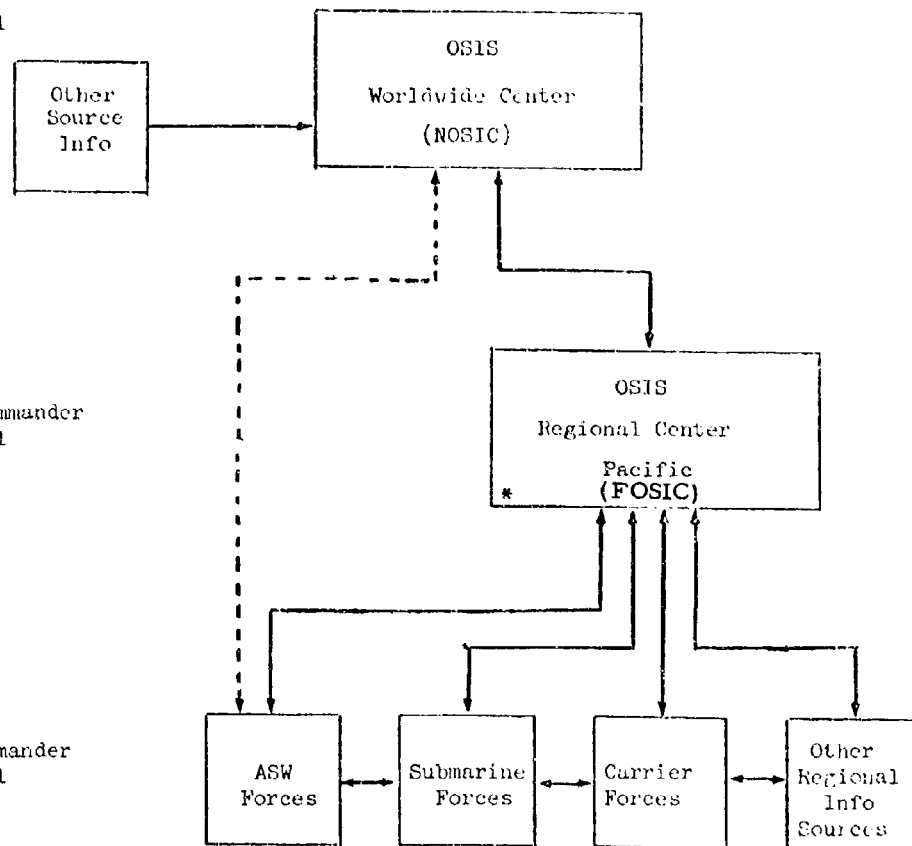
SECRET
(THIS PAGE UNCLASSIFIED)

National Level
 DOD Level

CNO Level

Fleet Commander
 Level

Type Commander
 Level



*Regional Centers planned for Atlantic, Pacific, Navy Europe, Western Sea Frontier

--- Flows when acting for Regional Center

Figure 2 - Organizational information flows

SECRET

IV. FUNCTIONAL INFORMATION FLOWS (Secret)

Although most information received by Centers will arrive by message on normal communications channels, provision must be included for incorporation of the numerous analyses, reports, and other data required for planning as contrasted to that for immediate operational use. Data arriving at the Centers will be received as formatted or non-formatted messages on the various communications circuits. This data completes communications processing, is decrypted, and is routed through data line terminals to the OSIS processors if in proper format. If received in unformatted state, an analyst must review, check, and format as necessary for insertion in the processor. It is expected that much classified information will be received, collated, correlated and entered in the data base without human intervention.

Functional information flows illustrating this process are depicted in Figures 3 and 4.

The machine processible data is comprised of that input received by the system which can enter the data base directly, since it has been processed and evaluated by a Fleet Center or other external agency whose capabilities are known.

Unevaluated formatted data may require substantial processing or analysis prior to entering the data base. Receipt of this data already formatted allows the system to locate, identify, and process discrete portions or elements of the entry without further manual preparation. Unevaluated non-formatted inputs cannot be machine processed without additional manual preparation including restructuring of substantive elements of the data.

The communications processor provides the point of entry and exit between Center processing systems and external communications. Functions of the communications processor include the categorization and routing of outputs, transmission of scheduled reports, maintaining records of transactions, etc.

UNCLASSIFIED

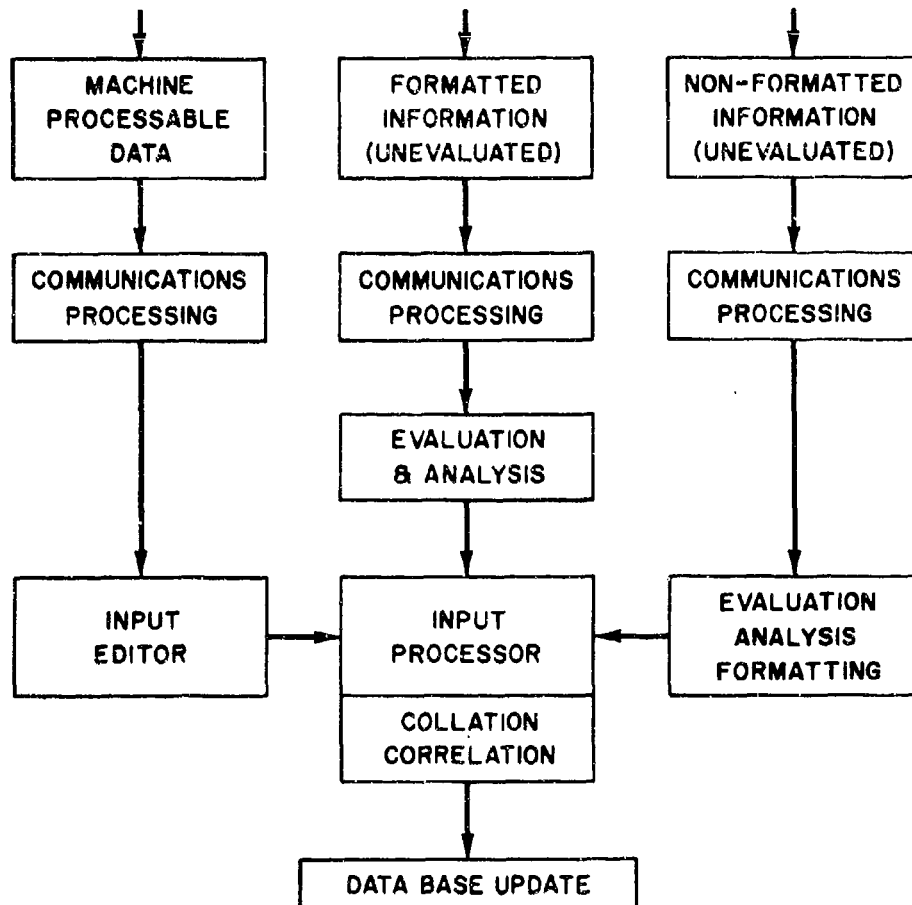


Figure 3 - Generalized system input information flows

UNCLASSIFIED

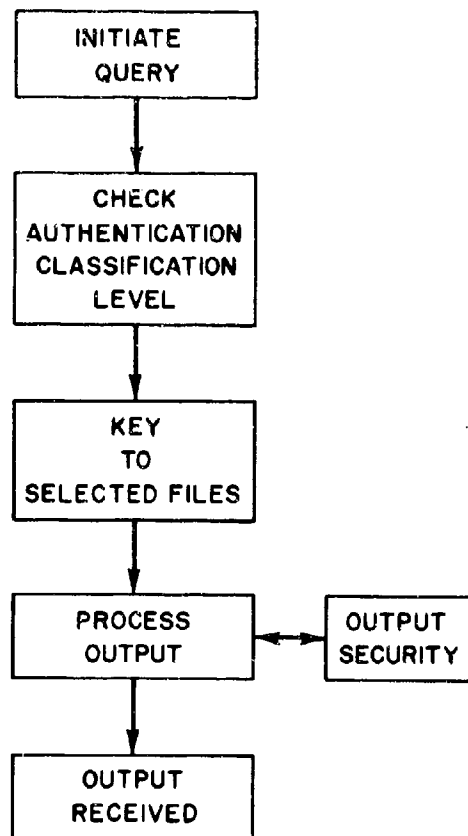


Figure 4 - Generalized system -
output information flow

UNCLASSIFIED

SECRET

V. SECURITY AND DATA CONTROL PROBLEMS (Secret)

Well defined physical and administrative controls are essential for the physical protection and the secure operation of the system. The security problems inherent in handling classified information in OSIS may be divided into categories of physical security, ADP hardware requirements, software requirements and personnel access. The Proposed Technical Approach (PTA)* has delineated some of the more pressing security problems in each of the above categories. These include the requirements that:

1. All computer systems handling classified information require restriction of physical access to qualified personnel, as well as provision of physical protection for the space containing the equipment. The PTA further specifies that there be no incidental access to the system data base, or its inputs or outputs, through electromagnetic or acoustic leakage.

Physical standards exist for the construction of physical facilities needed for the housing of classified equipments, together with specifications for construction of secure data links necessary for protection of input/output traffic during system operation. References for guidance on physical facility construction specifications as well as electromagnetic shielding requirements are included in Appendix A, Security Doctrine.

The provision of remote query devices to users and subscribers in widely separated areas significantly increases both the security problems and overall costs of the system. The costs of special security measures in existing command and control and intelligence

*PTA 35-15, Integrated, All Source Information Processing and Display System for Ocean Surveillance, April 1969.

SECRET

systems have resulted in extensive study efforts by the Department of Defense on reducing costs, while still providing the security protection required. The collocation of ADP facilities requiring security protective measures is being investigated by the Department of Defense (DOD) in order to improve effectiveness as well as reduce costs. Other pertinent studies on computer security have been undertaken under sponsorship of the Defense Science Board and the United States Intelligence Board. The results of all of these groups will provide a basis for updated DOD policy on security of classified information in automated systems.

2. Maintenance of security requires that only authorized users be capable of gaining access to the system. To accomplish the previously mentioned goals of the system, users having on line access to the system will be designated organizationally at the Fleet level and at the Navy Type Command (TYCOM) level. Individual ships and other activities may be designated as subscribers, and be eligible to receive off-line service.

Communications with remote terminals introduces the possibility of unauthorized users receiving access through switching errors. The likelihood of inadvertent switching errors in a switched communications network can be reduced during the technical design of the user and subscriber circuits; however, the system should be able to determine that any interaction taking place is with the proper party who has been granted the requisite degree of security access. Identification or authentication of the addressee by the system before providing an output may be feasible. Clearance of all users to the highest classification level contained in the system is an obvious, though costly approach to this problem. A more appropriate procedure for a system having users with varied levels of security access would

SECRET

be the use of authenticators or passwords for level of classification access and additional "keys" for entry to particular files within a classification level. The probability of compromise of authenticators and keywords is remote, and though these security procedures are technically feasible, authorities have not yet seen fit to authorize the operation of multi-level security access techniques. The use of cryptologic equipment and keying material represents an adaptation of equipment already approved for use in secure systems, and though expensive, might be justified on the basis of eliminating the additional authenticator - keyword technique.

3. All input messages incorporate classification "tags"; however, the system must also be aware of the classification of each output message, and the access limits of the addressee. Output messages should not be sent to a subscriber who does not possess access or "need to know" for the classification level of the message. Communications system errors could result in an encrypted classified message being sent to an unauthorized recipient in present day systems; however, the addressee will be unable to decrypt the message if it is in a higher classification code than that for which he has access. Possible approaches to satisfy this requirement include:

- a. Security verification programs, where queries having known responses are randomly inputted, and the system response compared with the correct response.
- b. Sufficient pre-operational testing in a closed environment to minimize probability of undetected hardware errors, and to insure thoroughly debugged software.
- c. Program monitor on all system operations. The use of audit trails.

SECRET

4. The system should not allow a user or subscriber to receive information for which he does not have access. In addition to the contents of an output message, there may be other relevant information stored in the system for which the user/subscriber may not be cleared. Should they be made aware of the existence of such information? Decisions on similar questions are not unknown to commanders operating in non-automated environments. Generally, such items should be "flagged" and routed to a human decision maker for resolution prior to transmission to the user/subscriber. It is believed that development of a meaningful policy in such an area where individual judgments prevail, would be more difficult than development of software support for the policy. An alternate approach is suggested, wherein FOSIC Commanders who are responsible for providing their subordinate commands all essential information required for tactical operations, will make the decisions on special information requirements of subordinate commands where ongoing operations are affected. The system security authority should provide staff assistance to the Commander in such instances.

5. The system response to inquiries may very well require more than the retransmission of single pieces of information from the data base. It is likely that sets of data, messages, or other information may be requested by the user/subscriber. Such a request requires that decisions be made on whether a higher classification is necessary for such a set of information, even though individual classification of each message in the set is known. Individual shipping plans may have no security restrictions; however, when all shipping plans for an area are assembled, the information may require a degree of classification. A similar situation exists when user/subscribers request information developed from the correlation of data from diverse sources, received by the system over a period of time.

SECRET

It becomes evident that the correct classification of system outputs is much more than a function of the classification of the inputs. The system must be considered to be the author of the data and thus has a responsibility for assignment of the proper security classification. Where this requires the judgment of a human decision maker there will be an increase in total system response time as a cost of providing proper security to the output. The increased time to provide proper security must be evaluated against the tactical need for a timely output, and the requirement that outputs must be properly classified and bear proper handling caveats.

An investigation of existing security doctrines has been undertaken which reviews the policies and rationale for assignment of security classification. Preliminary results are discussed in Appendix A. This review is yet to consider special categories of information, compendia of information, special handling caveats, and other information matters of a sensitive nature which require special clearances. A listing of Navy and Department of Defense security policy guidance directives is included in Appendix A.

SECRET
(THIS PAGE UNCLASSIFIED)

VI. FUNCTIONAL PROCEDURES FOR EFFECTING SECURITY (Unclassified)

The security problems involved in processing and analyzing classified information gave rise to the security requirements for OSIS, previously discussed in Section V. Generic information flows for the system were postulated in Section IV. Requirements for physical and electromagnetic security are discussed in current Department of Defense and Navy policy documents.

This Section will examine alternative procedures and techniques which could be employed to provide security in a multilevel system. Some of these techniques and procedures include:

1. The use of separate modes of operation. Privileged instructions contained only in executive and not available in other modes.
2. Hardware and software redundancy techniques which will continuously verify proper operation of the security features of the system, or provide interrupts on improper operations.
3. Segregation techniques which would physically isolate data of different categories or security classifications.
4. Identification and authentication techniques that will allow the system to verify the user's identify and levels of access to the system.
5. Incorporation of audit trails or logs of all classified operations.
6. Other techniques noted in Appendix B, which expand SOR requirements for incorporation in the Technical Development Plan.

SECRET

UNCLASSIFIED

A review of hardware requirements and software procedures for effecting security, including some procedures now being developed for intelligence systems, provides a framework for proposed work on the development of program modules for multilevel security in OSIS. Software techniques would include multilevel operations, the encryption of classified information, compartmentation techniques, and development of program modules for multilevel security.

HARDWARE REQUIREMENTS (Unclassified)

The design of a system that contains adequate security controls must consider the software components together with the hardware on which the software will run. Hardware features necessary in the development of a secure system should include provision for multiple modes of operation, interrupts, privileged instructions, memory bounds registers, and audit trails on all operations.

The processor should have at least two modes of operation, a control or executive mode and a user mode. The processor module will contain privileged instructions usable only in the control mode. Memory bounds registers should be incorporated which will provide comparisons for every memory address, and will restrict user access limits to those programs and data for which he has proper clearance. User programs are executed only in the user mode which contains only the unrestricted portion of instructions. Improper requests for or receipt of privileged instructions should result in an interrupt, requiring the attention of security monitor personnel before the program can continue.

User programs should be isolated from other programs in the system. The hardware mechanism for isolation includes memory bounds registers, with additional hardware checks to insure that memory

UNCLASSIFIED

addresses generated within the processor are in fact those allowed for the programs of a particular user. Other means of accomplishing this isolation might include length check registers or storage locks.

Some mechanism to provide memory protection is essential to OSIS. Unauthorized procedures or attempts to penetrate the system will likely generate an interrupt. These interrupts are the means for entry into the control modes, which may have resulted from numerous unsanctioned operating conditions, internal and external to the processor. Interrupts may be actuated by attempted memory bounds violations, improper remote terminal queries, power failure, occurrence of privileged instructions when in user mode, etc.

Illegal access within the system requires that the perpetrator execute privileged instructions assigned to security controls for the system. The execution of such instructions would require the system to initially be placed in the control mode of operation before allowing access for the execution of privileged instructions. Even though the above steps would require intimate knowledge of the system in order to gain access; additional protection for particularly sensitive security control instructions is desirable and could be accomplished by assignment of operation codes (or "flags") which must be correctly utilized in order to avoid an interrupt to the system.

An alternate approach to providing security would provide a sequence of instructions to be performed in preparation for the execution of the privileged instruction. Such a sequence would require entry at its beginning, and processing in its entirety, prior to accessing the privileged instruction. Errors or deviations at any step in the sequence would initiate interrupts by the system. This approach could be used with either a single or multimode system.

CONFIDENTIAL

MULTILEVEL OPERATIONS (Confidential)

Two techniques may be employed to ensure that personnel with security clearances have access to all information available in the system, within the limits of their clearance and need to know. The first of these techniques would be provision of security clearances for all system personnel to the highest classification level at which information is expected to be contained in the system. Computer systems operating in this mode are said to be "single level systems", or "single level security mode". In such a system every area of the computer system environment is afforded adequate physical protection, and personnel who have access to the computer environment may be granted access to the information being processed. Compartmentation by categories of information or segmenting portions of the data base is sometimes used in a single level system to restrict access to those individuals who have specific compartment clearances. A generic single level system employing compartmentation is depicted in Figure 5. Normal operations using such a multi-processor system would allow the remote terminals the use of only a single processing unit. Authorization from security management is required in each case before gaining access to other processors or compartments.

An alternative technique would be the operation of the system in a "multilevel security mode", or as a multilevel system. In this mode, some of the electrically connected equipment, e.g., remote consoles or displays, may be located in areas having lower levels of protection than the area of the central processor. Personnel having access to the computer may not have access to all categories of information being processed. Still another variation in the multilevel mode might include system operation in a multi-programmed mode, in which more than one category of classified information may be handled simultaneously. Operation in the multilevel security mode in OSIS

CONFIDENTIAL
(THIS PAGE UNCLASSIFIED)

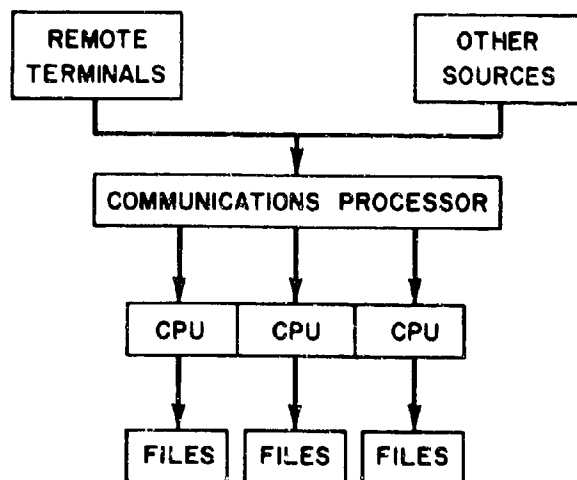


Figure 5 - Single level security mode
(Compartmented, multiprocessor configuration)

CONFIDENTIAL

requires the incorporation of special hardware and software features which will identify the user and his access level, maintain the integrity of the data, and will ensure that system outputs are routed only to the appropriate terminals. Operations in the multilevel mode give rise to the requirement for positive security measures which identify all users and allow control of access to the data base at the specified clearance level.

In either the single or multilevel modes, provision for the analyst to intervene in the system operation as needed for maintenance of security will be necessary. While the need for human intervention may be apparent in multilevel operations; many single mode operations may involve special handling procedures for sensitive information, physical disconnect provisions, and memory erase requirements, which will also remain primarily human operations even though effectiveness of the system may be impaired.

Figure 6 illustrates a sequence of information flow checkpoints for a generalized multilevel security system. Beginning with a requirement for personal identification prior to physical access to the area housing the equipment; the user must then identify himself to the system which will determine his access limits and provide this information to clearance level control. In addition to using an authenticator to enter the system, the user must employ a file access key in order for the system to determine which categories of files are to be accessed, based on the users need to know. The access key code also determines whether the user is authorized to insert information and modify the files, or only to read the accessed information. This procedure allows the user to query all files except SI within the level of his access authorization.

Access procedures for SI data are envisioned such that should the user be located at the National Center, and have access to all information

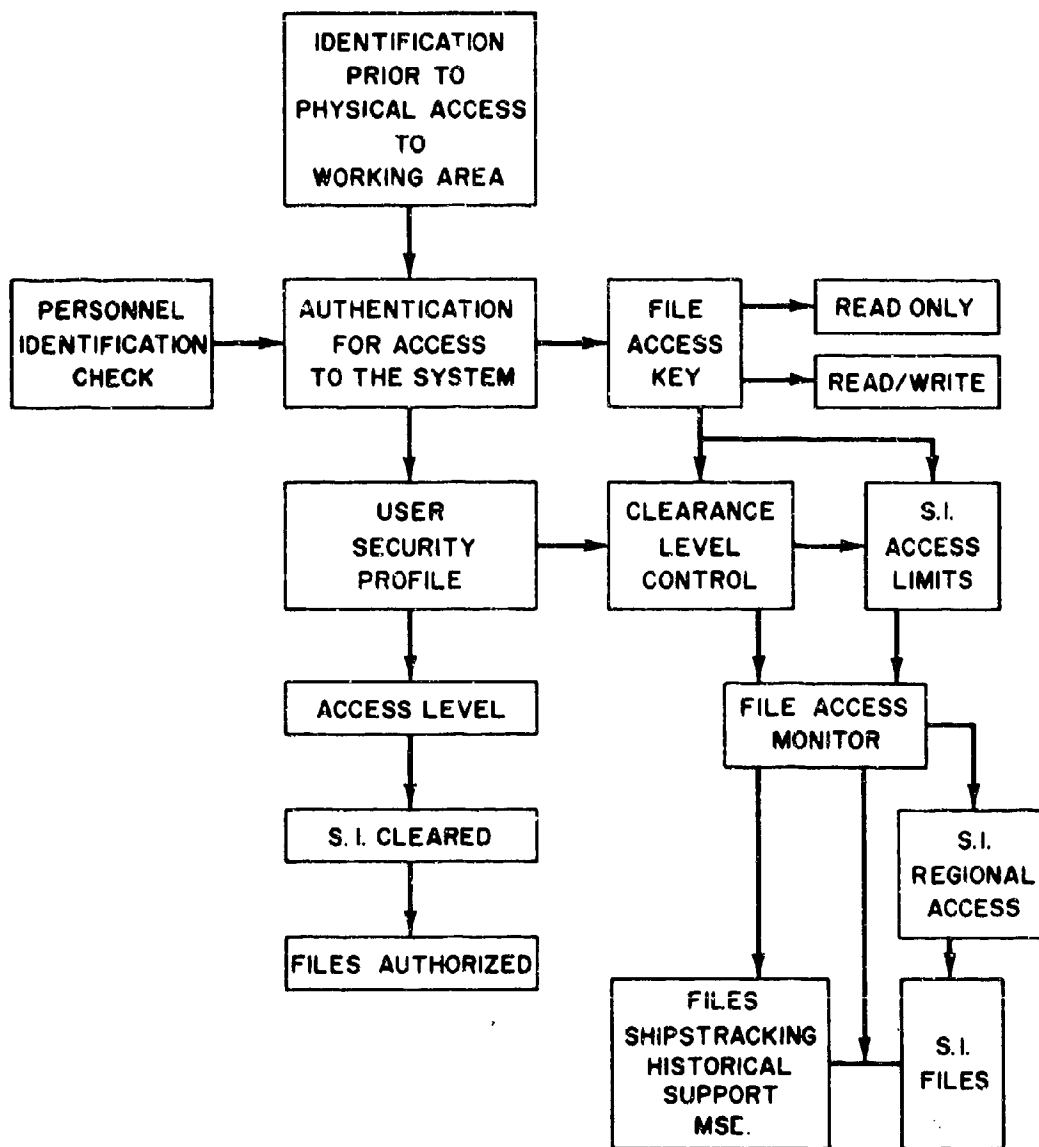


Figure 6 - Generic multilevel security information flows

CONFIDENTIAL

including SI, his access key would have identified his complete access authority, and all OSIS files would be available to him. If the user were located at a Fleet Center, it is postulated that he would have access to that Center's SI files only, and the file access monitor would so route his query, based on his file access key. Offline subscribers would not routinely have access to special category information (SI), however "sanitized" information may be available for dissemination at a lower classification level.

Current policy requires that groupings of information at various levels of classification be handled as if it were information of the highest classification level contained therein. Should that level be SI, there are additional physical security measures to be invoked. These include special marking of all hard copy, additional handling restrictions outside the secure area, machine lockout procedures as applicable when SI is being processed, and precautions to be taken in connection with reuse of storage media which has previously contained SI data.

The additional security requirements involved when handling SI leads to the consideration of other techniques for providing the user with necessary information in a more timely fashion. Assigning an arbitrary limit on the classification that may be used with certain categories of files which may require wide dissemination, e.g., information contained in "ships target activity" file would be assigned no higher than a Secret classification. Information of higher classification deemed essential would be provided separately when authorized by a human decision maker. Manual review of SI data and routine employment of sanitization techniques should reduce the operational user's needs for SI to the extent that it would be required infrequently.

CONFIDENTIAL

(THIS PAGE UNCLASSIFIED)

ENCRYPTION OF CLASSIFIED MATERIAL (Unclassified)

Classified information contained in a system may be encrypted and then treated as unclassified material. Such a procedure using internal encryption techniques would ensure the security of a classified system, even though uncleared users may have access to the system.

Department of Defense policy* requires the encryption of classified information when it is transmitted by electrical means. The feasibility of on-line encryption has been demonstrated. This technique would expand this existing capability and encrypt data stored in the system. All programs and all data files resident would be in encrypted form, and would be decrypted as they passed from storage to the processor for execution. The material would again be encrypted when it was returned from the processing unit to storage.

Access limitations would be accomplished by designating cipher systems for specific geographical areas. The establishment of discrete codes for application to the various levels of organization and degrees of classification would reduce access to only those users possessing the proper codes. For example, a shipboard terminal might have the capability of receiving and decoding messages up to the level at which the terminal is cleared; thus, a ship's terminal cleared to the Secret level would have a capability for decoding information at that or a lower classification level. Even though there is a possibility of some disclosure of information for which the recipient does not have a need to know, there would be no breach of security, but dilution of the "need to know" principle.

An alternative to wide use of encryption techniques is the encoding of selected categories of information, e.g., special intelligence within the system. The reduction in total encryption

*OPNAV Instruction 5510.82A, Security of Electrically Processed Classified Information.

UNCLASSIFIED

requirements makes such an approach attractive for further investigation.

Encryption of classified material is technically feasible, although it will result in an increase in costs and overall processing time in an operational system. The encryption approach may be subject to criticism on the policy making levels, on the basis that widespread use of encryption techniques provides a greater opportunity for security violations and penetration by inimical interests. The loss of a single code could compromise that portion of the data base. The adoption of encrypted techniques would tend to shift the principal source of insecurity from the machine to the human, where each user would represent a possible source of human error.

CLASSIFIED INFORMATION COMPARTMENTS (Unclassified)

Some degree of segmentation or compartmentation will be employed in the file structuring of any advanced system. Rather than a more conventional segmentation of information based on content, consideration was given to compartmentation of the information based on its level of security classification.

If OSIS is to provide services to a large number of unclassified or "low classification level" subscribers, consideration should be given to compartmentation of information by classification level. This approach would include compartments for each level of classification, with the files in each higher level classification compartment containing the data at the compartment classification level, together with access to the data in all lower classification level compartments. Thus the SI compartments would have access to all other data in the system; and intermediate level users would have access to all data at their level together with data of a lower classification.

UNCLASSIFIED

Classification level categorization is attractive when one considers that the data to be stored has been through a validation process, has been correlated, and assigned an appropriate security classification prior to entry into the data base. While compartmentation by classification level may satisfy security requirements; the storage of redundant information at the different levels, the added file complexity at each classification level, and the necessity for increased storage capacity, impair the effectiveness of this approach.

COMPARTMENTED SYSTEMS (Unclassified)

The compartmentation approach to handling security in automated systems is accomplished through the segregation of categories and classifications of information stored in the system, with varying degrees of access limitation placed on the different storage compartments.

The National Security Agency's remote access, multi-programmed system* called Rye has been processing classified data for over two years, and OSIS development may benefit from some of the procedures incorporated in this system. This system operates on a centralized, coordinated collection of ADP equipment including remote terminals for on-line computation, information storage, retrieval and processing. The system has a capability for processing and storing several compartments and levels of classified data simultaneously. Rye must provide not only security protection for the information, but must accomplish appropriate segregation of the data within the system according to its classification and special handling caveats.

The security structure for Rye is based on a composite of physical, machine, and communications security procedures. Physical

*NSA, Security Procedures for the Rye System.

UNCLASSIFIED

security procedures include the location of the equipment in a restricted area, special requirements for user identification, and proper clearances for those personnel who have access to the equipment. Physical security for remote stations is a responsibility of the organization for which the remote equipment is installed. Crypto-security is employed on dedicated communications links for all terminals located remote from principal computer installation.

The security measures incorporated in the system software would not be feasible without certain hardware protections incorporated in the computers (four UNIVAC 494's). This equipment may operate in any of four protection modes. These modes are:

1. The "worker" or guard mode with read, write, and jump protection. In this mode the central processor will not execute privileged instructions and will not read from, write into, or pass control to any core location lying outside the address limits described in the program. Privileged instructions include those capable of changing the internal functions or program lock-in registers.
2. The guard mode with write protection only. In this mode the system will not execute privileged instructions, and will not write in any core location outside the address limits of the program lock-in signature. This mode can read from or pass control to any core location.
3. The write protection only mode allows write in only within the address limits of the program lock-in register. This mode can read from or pass control to any core locations, and can execute privileged instructions.

UNCLASSIFIED

4. The executive mode, in which there is no prohibition on privileged instructions, and no checks on the addresses referred to by an instruction.

The normal operating state of the Rye system incorporates two kinds of programs, the worker and the executive. The executive controls logically all programs in the processor at a given time. The worker programs include all those other than the executive, and become active only at the discretion of the executive. The processors each have an executive program, though they share drum and peripheral core storage. One of the processors is tasked to allocate storage as required. As programs are activated in response to queries, data from storage will be passed to the worker program via the executive, and subsequent accesses must be approved by the executive before they are allowed. The worker program may transfer data freely within itself; however, it must go to the executive in order to communicate with any other area. Prior to providing an output to a remote terminal, its propriety is checked through the executive. When a worker program is completed, the executive terminates it, and clears the storage area occupied by the program. Since the executive monitors all data transfers when in the worker mode, any attempt to communicate outside the worker program is automatically noted by the executive.

For security purposes, four "objects" are identified to the system from remote access terminals. These are the user, the remote terminal, the program, and the permanent file. Information is the material being transmitted by the system, and as such is not included in the objects listed above. The user's access to the terminal is controlled by physical security procedures, and no further authentication is required by the system. The programs and files are identified through the system software, as is the remote terminal by the hardware.

UNCLASSIFIED

The system checks on the propriety of an information transfer by determining that the terminal and the user's access authority match the access level requirements of the program and classification of the requested file. The system approves queries on the basis of the security level of the "objects" (user, program, etc.) rather than on their names or designations. Security flags indicate the security level of all "objects", and may be used as general classification level indicators, or to indicate specific areas of compartmentation. A program's security flag is stored outside its core bounds. The executive will not allow a worker program to write outside its bounds, inasmuch as this would allow the program to change its security flag. A relation file describes the access relationships among security flags based on a relative ranking of the flags; whereby standard operating procedure, access is granted to queries from "objects" having equivalent or higher security-flag-ranking than those being accessed. In this system a worker program may communicate with a permanent file only if the worker program's security flag is higher or equal to the file security flag, and the query comes from a terminal authorized in the permanent file's access list. Flag relationships are also employed to authorize read and write in permanent files, as contrasted to read only authority. Temporary files allocated to worker programs are erased before being given to another program. The executive allows worker programs to receive input data from identified originating stations. When remote terminal call ups are made, the terminal's authorization to access the program is made by the executive program's security flag check.

Data entering a program takes on the security flag (classification) of that program. Data contained in a program is not downgraded by the system, since a program cannot write into a file having a flag lower than the security flag of the program (must at least be equivalent), nor can it output to a terminal having a security flag lower than the security flag of the program.

UNCLASSIFIED

Outputs from worker programs may be passed to stations having security flags equal or higher than the worker program's flag. Before the output is initiated, the worker program passes the designation of the receiving terminal to the executive, where the security flag comparison is made prior to outputting of the data.

The procedure for security flag interactions during the processing of a query into permanent files may be illustrated by the following sequence of activities:

- A program is called from file
- That program reads file #1
- That program writes in file #2
- That program creates file #3
- That program deletes file #4
- That program outputs to a remote terminal.

Let the security flag of the originator be ORGS, that of the program PROG, those of the files be F-1, F-2, F-3, etc. and that of the output terminal TERM. The relations among the flags are as follows:

- Program call-up : ORGS = PROG or ORGS > PROG
- Read File #1 : PROG = F-1 or PROG > F-1
- Write in File #2 : PROG = F-2
- Create File #3 : F-3 = PROG
- Delete File #4 : PROG = F-4
- Output : TERM = PROG or TERM > PROG

Since a program may access a file if its security flag exceeds that of the file, all data entering a program will take on the current security flag of the program. Information will not be downgraded in classification because a program cannot write into a file with a lower security flag. By the same token, data cannot be downgraded by passing from a higher security flag program to a lower value program. Human decisions are required to effect downgrading.

UNCLASSIFIED

Each console is driven by a single processor in the RYE system, more accurately, the executive in the processor. An active worker program may communicate with only one terminal, that terminal being a console belonging to the processor in which the worker program is resident. Worker programs may not communicate with other processors, nor may a worker program read from or write in any core location outside its own bounds. The worker program may only signal for an executive service. This service requires that the executive examine the worker program's request before any services are performed. Procedures are incorporated which abort any program that attempts actions which do not meet the executive security requirements. The worker programs are bounded and closely monitored and in themselves are unlikely sources of security improprieties. The executive, however, is a key link in system security, and any relaxation in executive control could lead to weaknesses in overall system security.

In summary, security is accomplished by providing information only upon authorization of its owner. The ownership and identification of files, programs, and remote terminals are represented by the security flags assigned. A security flag relation file denotes access requirements associated with each flag. Access may be granted on the basis of clearance level and need to know. Remote terminal access is based on terminal identity and not on the operator's identification to the system. Security flags and their relationships cannot be altered nor can the executive be altered from remote terminals. Only worker programs can be activated from remote terminals. Identity of the operator is determined by the organizational authority responsible for the terminal. The executive program and the hardware operational modes require worker programs to provide any outputs through the executive. Physically separate data links provide positive identification of remote terminals. These measures, together with the physical security precautions taken with all

UNCLASSIFIED

components of the system, including highest level clearance for all its personnel, comprise the Rye security structure.

Even though security requirements may be satisfied through the employment of security flags which determine who may access the various categories of information, the proper functioning of security procedures in advanced systems should be subject to a continuing security monitor program. This monitoring might be accomplished by a security verification program which simulates a user and inputs into the system a series of queries with known correct responses. The actual system responses can be checked with the verification-program-known responses at each step in the process, to insure that the system is in fact responding properly. When malfunctions occur, the operating personnel are alerted in order to take corrective actions. The system executive program should also be monitored for proper operation, through introduction of improper queries or attempts to gain access through the use of privileged instructions. A continuous detailed log of the operation of the security verification program should be maintained to assist in diagnosis of malfunctions, and to provide information for statistics on the system's operation.

PROGRAM MODULES FOR MULTILEVEL SECURITY (Unclassified)

The generalized multilevel security information flows illustrated in Figure 6 incorporate security check features similar to those in use in some of the automated systems which are currently handling classified material. Although present systems incorporate provisions for multilevel security operations, the use of a multilevel mode system has not yet been authorized, and as a result most users today are fully cleared for the highest classification contained within the system. There may be some access restrictions imposed on these fully cleared users, however, through the use of authorization keys or other means

UNCLASSIFIED

which are provided to gain access only to those files for which they have a need to know. OSIS may be required to begin operations with all users having full access to the system; however, early certification as a multimode system will require the continuing demonstration of its capability in multilevel operations. The program module approach should allow these operations in a benign environment until such time as the system is approved as an operational multimode system.

One problem with a multilevel system lies in the possibility that an operational decision maker will make the wrong decision, as a result of being provided with incomplete information. This problem has been previously noted, with reference to the security monitor being alerted when the system provides a limited clearance user only part of the information contained in the accessed files. The intervention of a human decision maker (security monitor) could introduce intolerable delays as the information processing load increases in the operational OSIS. For this reason, consideration must be given early in the development to provide techniques which make available all essential information needed in tactical operations, at a classification level that is available to the user. Sanitization of special information for distribution at a lower classification level will partially solve this problem. The longer term solution will lie in a comprehensive review of classification policies and possible redetermination of level of access requirements for subordinate tactical commands whose operations will benefit from the availability of OSIS information.

The Information Systems staff recommends a generalized software oriented approach to develop independent program modules which will support the multilevel security provisions of this or other systems which handle classified information. Physical and electromagnetic security requirements for systems handling classified material are provided by existing instructions which are referenced in Appendix A, and are not a part of this task.

UNCLASSIFIED

UNCLASSIFIED

Information flows in message receipt and filing are illustrated in Figure 7. Included are those modules required for meeting security requirements together with those needed for system operation whose design may be influenced by security considerations. It is recognized that classification is normally placed on messages by the originator; however, the extraction of data elements from the complete message during formatting may reduce or change the classification of individual data elements, particularly in those instances where a message source generates the degree of classification for the message.

Classification assignment rules will be generated where possible for various information sources and other identifiable categories of information. In addition to serving as a check to determine correct classification on incoming messages, the Classification Rules File should provide essential guidelines for the classification of outputs, and special handling caveats which may be necessary for proper handling of the material. This file will contain guidance for establishing an inferential or derivative classification on groups of data assembled or merged in special reports, analyses, and other system outputs. It is expected that this file will incorporate the decisions and modifications made by the system security monitor, when his intervention is required in the response to a query.

The Classification Rules File will also provide inputs for the classification downgrading program. The Navy downgrading and declassification policies provide initial direction, some of which may be adaptable to the downgrading of information contained in OSIS. Rather than using a time phased downgrading policy, which may not be applicable to OSIS data, this program must develop other techniques, such as matching of unclassified or reports of a lower classification with those of a higher classification. The results of this comparison

UNCLASSIFIED

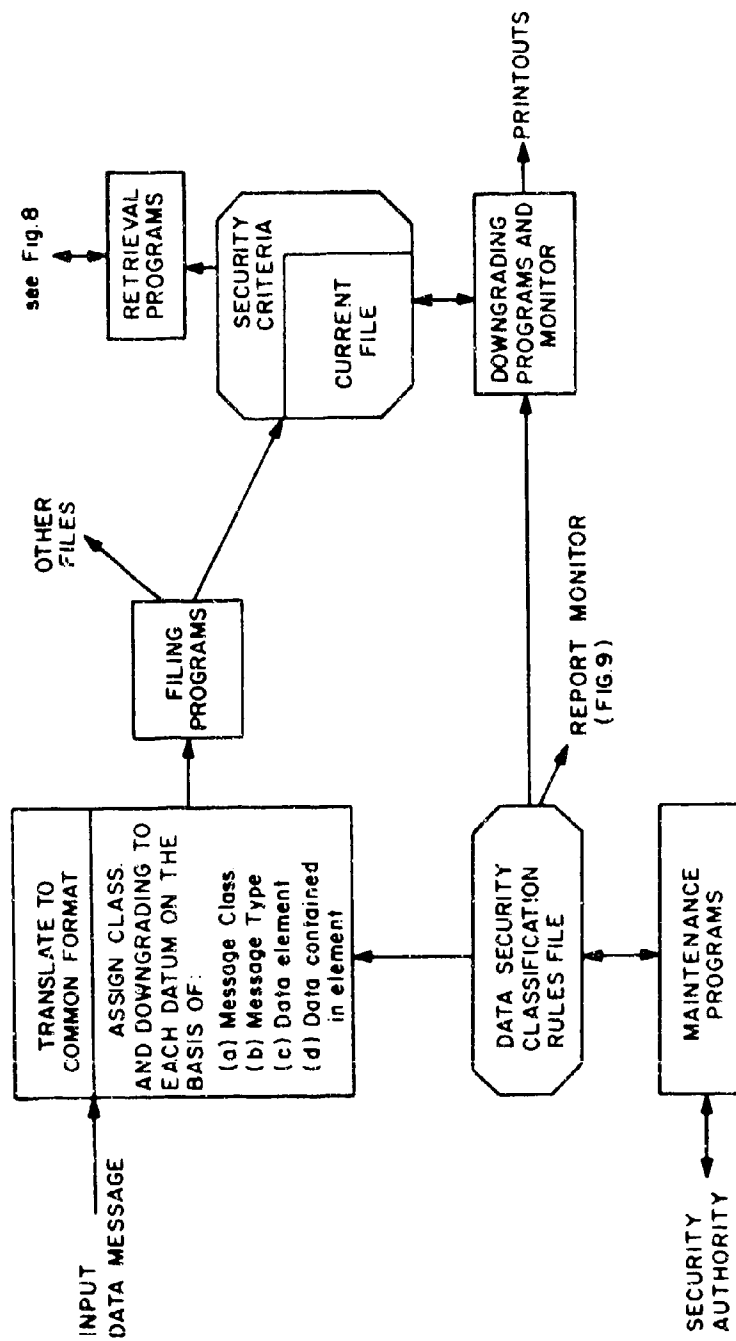


Figure 7 - Multilevel security message filing

UNCLASSIFIED

UNITED STATES GOVERNMENT
Memorandum

DATE: 7100-107
2 October 2003

REPLY TO

ATTN OF: Burton G. Hurdle (Code 7103)

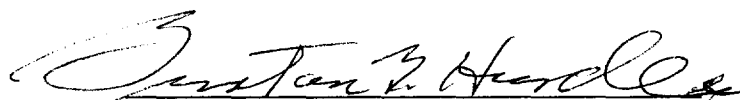
SUBJECT: REVIEW OF REF (A) FOR DECLASSIFICATION

TO: Code 1221.1

REF: ✓ (a) "OSIS Security Implications" (U), Paul Ashley, Information Systems Group, NRL Memo Report 2186, October 1970 (C)
(b) "Ocean Surveillance Sensor Identification" (U), Lawrence N. Morscher, Jr., Information Systems Group, NRL Memo Report 2190, December 1970 (S)
(c) "Laboratory Program Summary Reports for Naval Ordnance Systems Command" (U), Report Number 466173-85, November 1, 1969 (S)
(d) "Laboratory Program Summary Reports for Naval Ship Systems Command" (U), Report Number 466175-95, November 1, 1969 (S)
(e) "Laboratory Program Summary Reports for Naval Ship Systems Command" (U), Report Number 466175A-95, November 1, 1969 (S)
(f) "Laboratory Program Summary Reports for Naval Electronic Systems Command" (U), Report Number 466174-88, November 1, 1969 (S)
(g) "Laboratory Program summary Reports for Naval Air Systems Command" (U), Report Number 466172-99, November 1, 1969 (S)
(h) "Laboratory Program Summary Reports for Naval Air Systems Command" (U), Report Number 466172-99, November 1, 1969 (S)
(i) "Laboratory Program Summary Reports for Naval Ordnance Systems Command" (U) Report Number 466176, November 1, 1969 (C)
(j) "Laboratory Program Summary Reports for Naval Air Systems Command" (U), Report Number 466312, November 1, 1969 (C)

1. Reference (a) and reference (b) are reports on Project OSIS a study to develop an integrated Ocean Surveillance System including all appropriate technologies. The system was never developed. Reference (c) through reference (j) are a collection of NRL program summaries associated with the project.
2. Reference (d) and (g) contain sensitive material and should remain classified as indicated.
3. The technology and equipment of reference a, b, c, e, f, h, i and j have long been superseded. The current value of these papers is historical.

4. Based on the above, it is recommended that references a, b, c, e, f, h, I, and j be declassified and released with no restrictions.



BURTON G. HURDLE

NRL Code 7103

CONCUR:

Edward R. Franchi 10/3/2003

E.R. Franchi

Date

Superintendent, Acoustics Division

CONCUR:

Tina Smallwood 10/7/03

Tina Smallwood

Date

NRL Code 1221.1